UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

HANAN ELATR KHASHOGGI, Plaintiff, v. NSO GROUP TECHNOLOGIES LTD. and Q CYBER TECHNOLOGIES LTD., Defendants.	Case No. 1:23-cv-779-LMB-LRVVAED

DECLARATION OF BILL MARCZAK

I, Bill Marczak, pursuant to 28 U.S.C. § 1746, hereby declare as follows:

1. I obtained my PhD in Computer Science from the University of California at Berkeley, and I currently reside in El Cerrito, California.

2. I am a Senior Researcher at the Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research and development at the intersection of information and communication technologies, human rights, and global security.

3. In my role at the Citizen Lab, I conduct research into government use of spyware and hacking tools to carry out espionage against journalists, dissidents, and civil society targets. "Spyware" refers to any software or hardware component that is installed on a target's electronic device, without their consent, to facilitate third-party access to data stored on the device, or to the device's functions (e.g., turning on the device's microphone to record audio in the device's vicinity). I focus on companies that sell spyware and hacking tools and services directly and

exclusively to governments, including NSO Group. Companies in this industry typically represent that their spyware products are intended to be used by governments exclusively for tracking serious organized crime and terrorism, though the reality of their use is somewhat different.

4. In 2016, I co-published the first public report on NSO Group's Pegasus spyware. The report, entitled "The Million Dollar Dissident," describes how I clicked on a Pegasus installation link sent via SMS to United Arab Emirates (UAE) activist Ahmed Mansoor (who was immediately suspicious of the SMS and forwarded it to me for analysis), and obtained a full copy of NSO Group's Pegasus spyware. The report received substantial media coverage at the time, as it was the first publicly documented case of a "zero-day remote jailbreak" used to install spyware. A "zero-day remote jailbreak" is a chain of zero-day exploits (malicious code that takes advantage of unintentional software vulnerabilities unknown to the software's developer) designed to subvert the iPhone's security features and permit the installation of apps on the device not approved by Apple. We at Citizen Lab shared this code with Apple, who issued an emergency update (iOS 9.3.5) to fix the specific flaws exploited by Pegasus in this case.

5. Following "The Million Dollar Dissident," NSO Group reportedly released a new major version of Pegasus ("Pegasus 3"). NSO Group continues to regularly release new versions of Pegasus containing new zero-day exploits, designed to install Pegasus on the latest iPhone and Android devices. Since "The Million Dollar Dissident" report, I have examined phones belonging to numerous civil society targets around the world, in an effort to determine whether they have been compromised with Pegasus. While I have authored multiple reports chronicling the abuse of Pegasus around the world, these findings are typically based on *forensic traces* of Pegasus infection (i.e., partial fragments of Pegasus code, artifacts in system logs showing

communication with Internet servers used by Pegasus, or other evidence that Pegasus ran on a device). NSO Group implements several layers of safeguards in an effort to prevent security researchers like me from recovering full samples of Pegasus.

6. Around July 23, 2021, I began a forensic analysis of Hanan Khashoggi's devices in order to determine whether the devices were targeted or hacked with Pegasus, or other types of spyware.

7. Thus far, I have spent approximately 40 hours performing research and analysis into Mrs. Khashoggi's devices. I attest that the value of my time and services exceeded $5,000 for the examination and investigation of Hanan Khashoggi's devices.

8. My analysis concluded that Mrs. Khashoggi's Android phones had been targeted by Pegasus multiple times beginning on November 8, 2017, and extending through at least April 22, 2018. On December 21, 2021, I shared the conclusions of my analysis with Mrs. Khashoggi and her attorney, Randa Fahmy.

Findings of My Analysis

9. On April 22, 2018, a user manually typed in a URL associated with a Pegasus installation website into the address bar of the Chrome web browser on one of Mrs. Khashoggi's Android phones and visited this URL. This occurred shortly after the phone was carried into the United Arab Emirates (UAE). This is consistent with Mrs. Khashoggi's reported detention upon arrival in the UAE, indicating that authorities likely would have had physical access to her device.

10. As a result of visiting the URL, Pegasus installation commenced on Mrs. Khashoggi's Android phone, and the Chrome web browser on her device successfully sent 27 pieces of telemetry to the Pegasus installation server over a period of 40 seconds, updating the

server on the progress of Pegasus installation (the installation of any spyware is a complex process involving multiple steps). Because modern versions of Pegasus communicate this telemetry using numbers whose meaning is opaque to third parties (e.g., "204", as opposed to a legible message like "exploit succeeded"), it is not currently possible to understand from this information alone whether the final Pegasus payload was installed on Mrs. Khashoggi's device. Additionally, I have not noticed the presence of (nor the conspicuous absence of) indicators that would be associated with the final Pegasus payload on Mrs. Khashoggi's phone. Phones are not typically designed to preserve log information for such an extended period of time, and forensic traces of spyware discovered far in the past are often due to "luck" (e.g., particular usage patterns of the device that lead to old log fragments not being deleted or overwritten).

11. However, based on the analysis described in my forensic report, and my prior studies of the Pegasus software suite, the likelihood that the Pegasus infection succeeded is high. In my experience, if a device does not support installation of the Pegasus spyware, for example because the particular device model or installed software versions are not vulnerable to exploits employed by Pegasus at the time of infection, then this will often be detected *immediately* when a Pegasus installation URL is visited, and the user will be redirected to a benign website before installation commences. Of course, more complex failure cases can arise during Pegasus installation, but an adversary with physical access to the phone could remedy certain issues that might cause Pegasus installation to fail (such as by uninstalling an app conflicting with Pegasus, or by changing various settings on the device) and then make a second installation attempt by visiting a second link shortly thereafter. There is no evidence of a second installation attempt around the same time.

12. In November 2017, six separate Pegasus infection attempts were made through SMS text messages sent to Mrs. Khashoggi's phone. A similar attempt was made on Mrs. Khashoggi's second phone in April 2018. Based upon my preliminary review, I am unable to state with certainty that those attempts resulted in installation of the final Pegasus payload, for the reasons stated above, but also have no evidence to believe they were not successful.

13. On July 10, 2018, the WhatsApp application on Mrs. Khashoggi's phone experienced two crashes. The nature of these crashes appears suspicious. The crashes occurred while WhatsApp was handling multiple incoming video call requests from a Cypriot number unknown to Mrs. Khashoggi. The WhatsApp application further experienced several more events from the Cypriot number between August 1, 2018, and October 14, 2018. The WhatsApp crashes appear consistent with a "zero-click" exploit deployed against WhatsApp users by NSO Group customers via a WhatsApp video call request.

14. In May 2019, WhatsApp released a public disclosure regarding this exploit as well as an updated version of WhatsApp containing a fix for the underlying vulnerability. In October 2019, WhatsApp sued NSO Group regarding the exploit. WhatsApp's lawsuit states that NSO Group customers deployed the exploit using call requests initiated from WhatsApp accounts with phone numbers registered in "Cyprus, Israel, Brazil, Indonesia, Sweden, and the Netherlands," and that WhatsApp accounts used to deploy the exploit were registered as early as January 2018. The exploit did not require the targeted user to take any action (such as accepting or declining the call) for Pegasus spyware installation to succeed.

15. Further, I am aware that representatives of NSO Group have made the dual claims that the Pegasus spyware 1) generally cannot be installed on phone numbers associated with the United States (for example, if an installation attempt is issued for a phone number, and that

phone number has a country code of +1 – a telephone country code used by various countries in North America and the Caribbean, including the U.S. and Canada – as well as an area code assigned to the U.S., then the attempt should generally be denied by the Pegasus system), and 2) is generally ineffective or otherwise non-functional within the geographic boundaries of the United States. Though, the precise application of these restrictions and the availability of exceptions remains somewhat unclear. Such restrictions do not appear to be applicable in certain cases, for example, a product demonstration of Pegasus to the United States Federal Bureau of Investigation (FBI) cited in WhatsApp's lawsuit and reported in the New York Times involved the use of the spyware against a +1 phone number with a U.S. area code.

16. Additionally, as no public analysis of a full Pegasus spyware sample has been published since 2016, it is not possible to conclude whether or not recent versions of Pegasus contain technology designed to prevent its use within the geographic borders of the United States, whether such technology existed during the time period of Mrs. Khashoggi's targeting, whether such technology would have been applicable to all of the various manners in which Mrs. Khashoggi was targeted, and if so, whether such technology was likely to be effective in all cases.

17. While such technology, if implemented and consistently enforced, could theoretically block most usage of Pegasus in the United States, in my professional opinion, it would be very difficult, if not wholly impossible, to guarantee that *no data* would *ever* be transmitted by Pegasus after a target hacked with Pegasus abroad entered the geographic bounds of the United States.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Dated: October 13, 2023

Bill Marczak